CHAPTER 1

Critical Infrastructure Protection Strategies: The Direction and Intent

Introduction

Comments of the Honorable John O. Marsh[1]

Secretary John O. Marsh introduced the session by setting a framework for the evaluation of the current requirements for critical infrastructure protection. He recommended that the participants direct their attention to the October 1997 report of the President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures*.[2] The commission, convened in the aftermath of the bombing of the Murrah building in Oklahoma City, dealt primarily with the cyber-security issues surrounding infrastructure protection. Its findings would lead directly to the development and promulgation of Presidential Decision Directive 63 (PDD-63). Over time, the concept would broaden from the focus on cyber-security to include both cyber and physical infrastructure, as it became apparent that they were inextricably linked, with the protection of each integral to the protection of both.

The 1997 Commission Report presents two key conclusions: 1) that the law has failed to keep pace with technology, and 2) that neither the private nor the public sector is aware, or properly appreciative of this failure. The report also introduced the concept of "key sectors" to the public agenda—numbering over time between seven and thirteen, depending on which study or document is being referenced.[3] Focusing

[1] Secretary Marsh's comments were transcribed after the session.

[2] A copy of the report is available at <http://www.loyola.edu/dept/politics/intel/PCCIP_Report.pdf>.

[3] Homeland Security Presidential Directive 7, "Critical Infrastructure Identification, Prioritization, and Protection," lists thirteen "critical infrastructure" sectors and four "key resource" sectors.

on these sectors—energy, transportation, water, et al—provides us an entry into identification, prioritization, and protection issues.

The report recommended reaching out to the private sector, which poses a whole new set of issues. The Federal system, particularly defense, as well as State and local governments, is absolutely reliant on the infrastructure provided through the private sector. However, the Federal government has (to date) failed to devise a procedural mechanism for coordination with that sector. The most effective efforts have been in the financial sector through the implementation of their Information Sharing Analysis Centers (ISAC), but other ISACs in other sectors have not been nearly as successful. The Federal government will need to develop new modalities for coordination and cooperation, particularly in the area of statutory protection for private industries. For example, Secretary Marsh pointed out, efforts for dealing with the Y2K crisis would have been exponentially more difficult, if not impossible, had it not been for the United States Congress' suspension of elements of the Anti-Trust Law and the Freedom of Information Act. Similar measures may be necessitated in other CIP issues. However, Secretary Marsh warned that in the process of effecting that protection, the concurrent protection of individual liberties and individual privacy must remain in the forefront of our thinking.

Formulating Strategies for Critical Infrastructure Protection

Professor Bert B. Tussing

Professor of National Security Issues
Center for Strategic Leadership
U.S. Army War College

The United States Army War College, like its sister institutions in Newport, Maxwell, and Washington, devotes no small amount of attention to the study of Strategy. A significant amount of that study is directed at the unique concerns of military strategy; but a key lesson—perhaps the key lesson that we try to drive home with our students—is that military strategy is only a component of a larger Grand Strategy, and must be developed in support of and subordinate to the same. Failing to do so will, at best, lead to inefficiencies; at worst, it will lead to an application of the armed forces that is separate from and potentially opposed to the interests and policies of the Nation.

I would like to suggest that the same dangers could evolve within other sectors of the Federal government, whether addressing diplomatic policy, economic initiatives, or directives surrounding our law enforcement agencies. And the same can be said for our efforts to provide for homeland security. In that light, this paper is devoted to taking the reader down the same twisted paths we lead our students in discussing strategy and how it is developed. It will introduce the reader to the Strategy Formulation Model used as a framework for analysis at Carlisle and, through that framework, will examine the tenets and motivations that go into making the Nation's Grand Strategy. In the process, I hope to directly and indirectly portray the applicability of this model to an examination of the evolving strategies for homeland security in general and CIP in particular.

Strategy in General

Let's try and begin from a relatively straightforward concept of what is meant by Strategy. Strategy is all about how leadership will use the power available to a given state to exercise control over sets of circumstances in order to achieve objectives that support the state's interests. Strategy provides

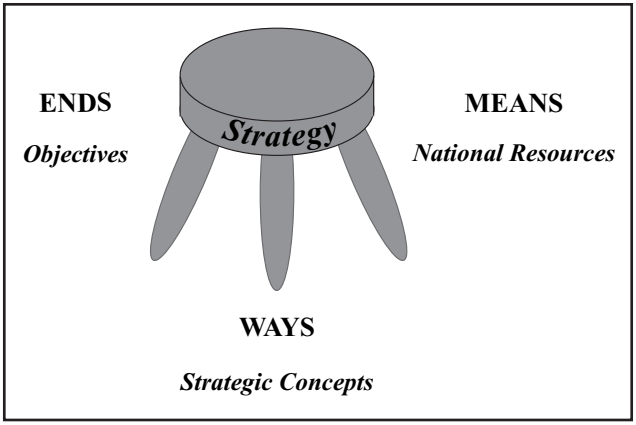

Figure 1: Three-legged stool model for strategy

direction for the persuasive, or coercive use of this power to achieve specified objectives. Breaking down that relatively simple definition, Strategy becomes an examination of how (read "concepts" or "ways") a nation will apply power (read "resources" or "means") to accomplish its objectives (or "ends"): the classic "ends, ways, and means" portrayal. As students find themselves working through different "layers" of strategies (for instance, when examining "implementing strategies" that support "senior strategies") they will sometimes discover that the "way" that supports one strategy becomes the "end" of another. A clear example of this transformation applicable to discussions surrounding homeland security can be seen in the relationship between CIP and the National Strategy for Homeland Security (NSHS); protecting critical infrastructure and key assets is a "way" toward the NSHS "end" of "reducing America's vulnerability to terrorist attacks." However, it is clear that in the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets this "way" is a desired "end," in and of itself.

Similarly, one strategy's "means" may be another strategy's "end," such as in the relationship between the Defense Industrial Base (DIB) and the National Military Strategy (NMS) it supports. Whatever the case, experience has taught us that this "ends, ways, and means" analysis is an effective tool in conveying our concept of strategy.

In fact, since at least 1989, by way of a series of lectures presented by the venerable Colonel Art Lykke, U.S. Army (Retired), the War College has portrayed this model for strategy by means of a three-legged stool (see figure 1). The model not only portrays the elements required to uphold a strategy, but it conveys the notion of a necessary balance in these elements that must be maintained for the strategy to be successful.

Of course, this perfectly balanced strategy is only conceptual. There will seldom be a time when all of the resources needed for a given end are available to us, or when the perfect concept for their application has been derived. There will be times when, in order to execute our strategy, we will have to obtain additional resources, re-work our concept, or redefine our required ends. Or, we will have to live with the existing imbalance. Doing so introduces the element of risk (see figure 2).

Risk explains the gap between what is to be achieved (ends) and the concepts (ways) and resources (means) available to achieve it. The greater the gap is between these elements (portrayed as the angle in figure 2's diagram), the greater the risk. Where risk is determined to be unacceptable, the strategy must be revised. Options to reduce risk would typically include changing the objective, changing the concepts, increasing the resources, or reducing the threat.

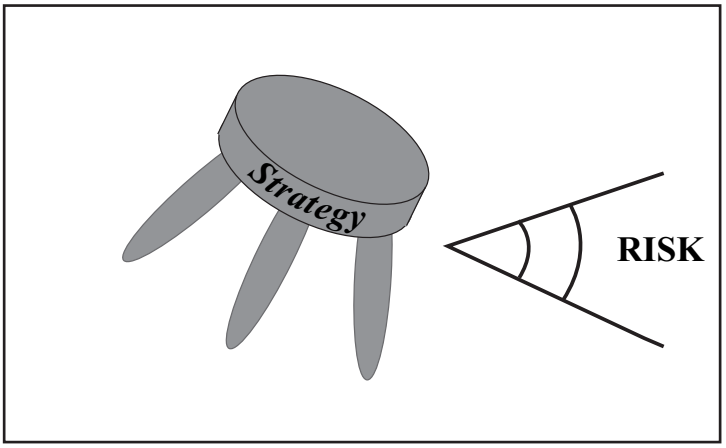

Figure 2: The Element of Risk

A Strategy Formulation Model

Having established an "ends, ways, and means" mindset, I would like to move on to an examination of the Army War College's Strategy Formulation Model (see figure 3). The model is intended to portray a progressive approach to building a strategy that inherently weaves a common direction and uniformity of purpose. The process begins with an affirmation of our National Values. These are what we hold to be the legal, philosophical, and moral basis of the American system. They embody principles such as liberty, equality, the rule of law, and opportunity for all people. In the National Security Strategy (NSS), they are specifically embodied in goals calling for "political and economic freedom, peaceful relations with other states, and respect for human dignity."[4] Viewed against current domestic and global needs, these values form the foundation of our core National Interests.

National Interests basically describe the Nation's perceived needs and aspirations, largely in relation to the rest of the international community. These are what motivate us to action, determining much of our involvement with the rest of the world, providing a focus for those things that need protection in that world, and generally serving as the starting point for defining national security objectives and then formulating national security policy and strategies to achieve and maintain those objectives. In order to help us focus on what we hold to be our national interests, we divide them into Categories and Intensities. At the Army War College, national interests are grouped into four broad categories:

- Defense of the Homeland
- Economic Well-Being
- Favorable World Order
- Promotion of Values

Within each of those categories we assign intensities—Vital, Important, or Peripheral—basically designed to answer the question: "What happens if this interest is not realized?" These delineations allow

[4] The White House, The National Security Strategy of the United States of America, Washington, D.C., September 2002, p 1.

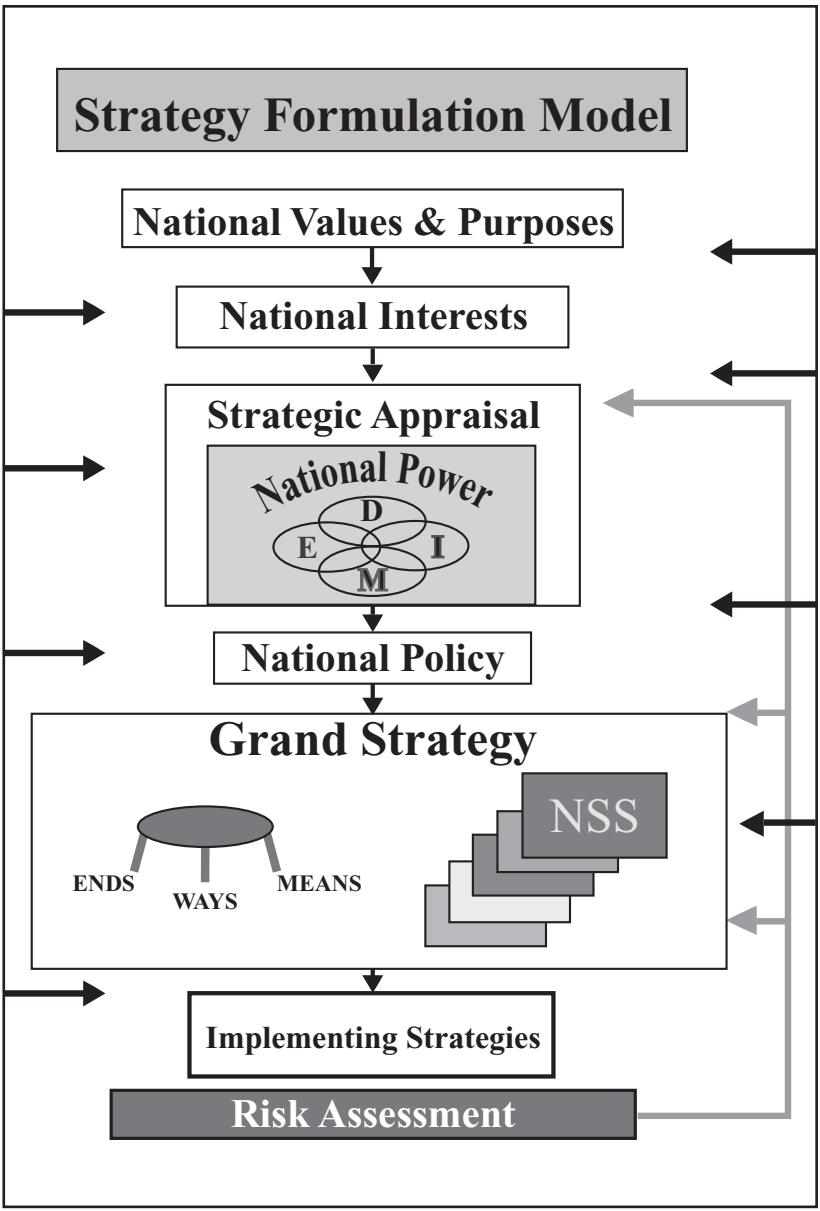

Figure 3: The Strategy Formulation Model

Intensity of Interests

- **Vital: Those interests directly connected to the survival and vitality of the Nation.**
  - *If unfulfilled, will have immediate consequences for core national interests.*
- **Important: Those interests affecting our national wellbeing or that of the world in which we live.**
  - *If unfulfilled, will result in damage that will eventually affect core national interests*
- **Peripheral: Those interests which, if unfulfilled, may result in damage that is unlikely to affect core national interests.**

Figure 4: Intensity of Interests

us a means of assigning priority or criticality to our interests by assigning a sense of immediacy (See figure 4).

This eventually takes on great importance as we are forced to make decisions surrounding resources available to be used against our desired ends. Returning again to the current National Security Strategy (NSS), our national objectives include (for example) championing aspirations for human dignity, strengthening alliances to defeat global terrorism, working to prevent attacks against us and our friends, and transforming America's national security institutions to meet the challenges and opportunities of the twenty-first century.[5]

The next step, frequently a concurrent step in our model, involves conducting a Strategic Appraisal of the domestic and international environment. This begins with an assessment of our National Power, that strength or capacity of a nation to influence the behavior of other nations (or—of growing importance—non-state actors) in accordance with its national objectives. At the Army War College, students are

[5] Ibid

taught that there are two distinguishable components of national power: the Elements of National Power, and the Instruments of National Power. Elements of Power include both natural and social determinants. Natural determinants, such as geography, natural resources, and population, are relatively stable, and in essence provide the raw material by which the power of a nation is fashioned. Perhaps that relative stability is what causes us to focus more on the social determinants—Diplomatic, Informational, Military, and Economic—which are by their nature subject to constant change. Taken together, these determinants provide the "means" to achieve our national objectives and to secure our national interests. Our instruments of national power are the policy options and other "tools" by which we exercise these means. These can range from components of our military forces, to trade agreements, to elements of the fourth estate.

The nature of our examination may vary (for instance, are we examining the overall National Strategy, a component of that strategy, or a separate "supporting" strategy?), but the Strategic Appraisal is generally approached as a four-step process:

Step 1–Determining Interests (by Category and Intensity)

Step 2–Identifying and Assessing Challenges

Step 3–Comparing our appraisal to the NSS

Step 4–Developing Policy Recommendations

The first two steps are clearly aligned with concerns over prioritizing needs and the ability to provide for those needs. Similarly, the third step is directed to maintaining a proper focus by ensuring that the direction of effort is aligned with priorities already prescribed in the Nation's "Grand Strategy," the NSS. While this step pays homage to what is held to be the "senior" strategy for our Nation's overarching security concerns, it is representative of the same type of scrutiny that must be applied to any strategy, or component thereof, that is developed in support of another strategy.

Step 4 alludes directly to the next step in the formulation model, the development of National Policy. This is basically the guidance provided by our national leadership towards the formulation of a "Grand Strategy" designed to secure our national interests.

National policy can be thought of as a broad course of action defined variously by official documents, directives, and other statements of guidance delivered by the government at the national level in pursuit of national objectives. It defines a vision of where the country should be in the pursuit of its national interests.

Joint Publication 1-02, The Department of Defense Dictionary, holds the NSS to be synonymous with both National Strategy and (as depicted in our Formulation Model) Grand Strategy. The accompanying definition for Grand Strategy basically brings our model as addressed to this point together neatly:

> …the art and science of developing, applying and coordinating the instruments of national power (diplomatic, economic, military, and informational) to achieve objectives that contribute to national security.

In his lecture on Grand Strategy and National Security, Dr. Robert Dorff of the Army War College faculty refers to Grand Strategy as,

> …the use of all U.S. national power in peace and war to support a strategic vision of America's role in the world that will best achieve the Nation's core objectives.

In examining these two definitions, the confluence of interests, objectives, power, and policy are clearly discernable. But this is not meant to imply an end to the discussion. Returning to the model finds the next step, Implementing Strategies (sometimes referred to as Supporting Strategies), which may be thought of as serving elements of the larger strategic end. At the Army War College, the implementing strategy of the NSS that most quickly comes to mind is the NMS; but other examples could include the Department of State and USAID Strategic Plan, the U.S. Department of Justice Strategic Plan, and the NSHS. Each of these, in turn, could have additional implementing strategies of their own.

The final element of our Strategy Formulation Model is Risk Assessment. As depicted in figure 3, we are led to examine risk assessment from two separate perspectives. The first has to do with the inherent risk element contained in our "ends, ways, and means" approach to strategy. Risk, as pointed out in the model, is inevitable; our task lies in choosing where we accept risk and managing it, rather than allowing it to manage us. The second perspective is directly related, in that we are obliged to assess

TESTS FOR STRATEGY

- **Suitability – will its attainment accomplish the desired effects (relates to Ends)**
- **Feasibility – can the ends be accomplished with the means available (relates to Ways)**
- **Acceptability – are the consequences of cost justified by the importance of the desired end (relates to Ways/Means)**

Figure 5: Tests for Strategy

risk through each and every step of our strategy formulation process. As new elements of risk are encountered, as new threats present themselves, a strategy must adjust if its objectives are to be achieved.

In addition to Risk, and borrowing from the old Naval War College Green Book, Sound Military Decision,[6] the Army War College prescribes three "tests" for any given strategy: Suitability, Feasibility, and Acceptability (see figure 5). Suitability is tied directly to an assessment of whether or not the designated ways and means will achieve the desired ends. In a lecture to Army War College students examining the balance between ends ways and means, Dr. Dorff declared succinctly: "Ends matter, and ends matter most."[7] A set of concepts and resources devoted to ends that are in opposition to national policy, no matter how efficiently applied, is counterproductive in the gravest sense. Similarly, Feasibility must be examined as the ultimate "reality check" for the strategic planner; concepts without resources would amount to Blitzkrieg without tanks and trucks. Finally, strategies should be judged against the criteria of Acceptability, balancing not only the cost of expenditure in resources, but likewise the

[6] See the Naval War College Review, May-June 1979, pp. 11-21, "Strategy-The Theory and Application," by Rear Admiral Henry Eccles.

[7] Dr. Robert Dorff, "War and Politics: Introduction to Grand Strategy and National Security," lecture Carlisle Barracks, PA, U.S. Army War College, 22 August 2002, cited with permission of Dr. Dorff

potential cost of abandoned principles. Draconian measures initiated in the name of security, for instance, would not be borne long by a free and open society.

The task of strategy formulation is imposing enough under this model to this point; but thus far we have viewed that model as basically self-contained. Ours is not a self-contained world. On the contrary, a rational model will be constantly affected by a series of influences from both the global and domestic fronts that will cause the strategist to reassess and reevaluate the construct and components of his strategy along every stage of its development (see figure 6).

These two sets of external factors may occasionally coincide in their effects on the National Strategy, or they may present it with markedly conflicting purposes; but their influence will be perpetual and their demands against that strategy inescapable. These "external demands" will frequently come at the hands of our allies, our friends, and even our own citizenry; or they may come from a deliberately malevolent enemy whose values, interests, and objectives lie in direct opposition to our own.

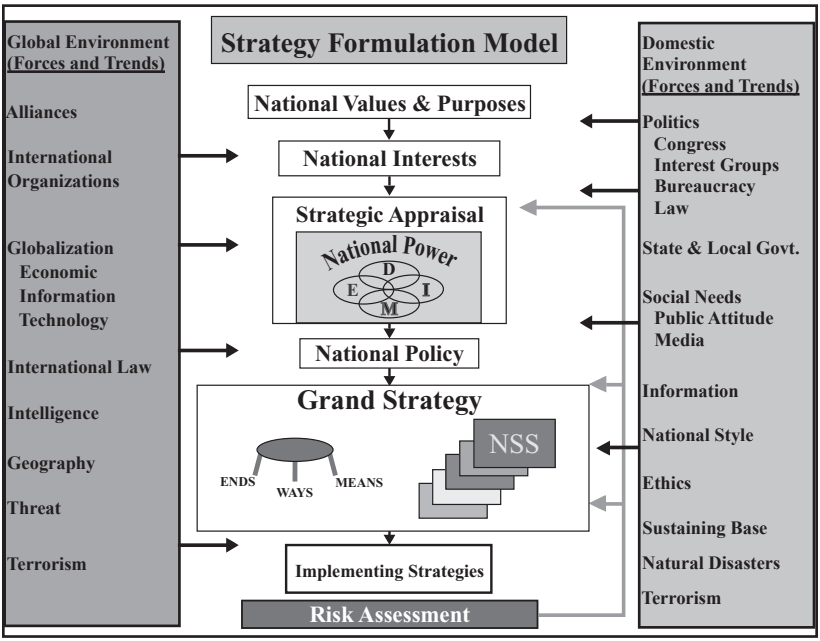

Figure 6: Affects on the Formulation of Strategy

Such external influences serve to remind us that a strategy is a framework, not a blueprint. It is a dynamic mechanism that helps us to define our interests and objectives and our options to achieve the same, but it is not a "plan." Particularly when faced with contradictory interests and wills, it will require constant re-evaluation. It is a process for systematic analysis.

Critical Infrastructure Protection Strategies

Having gone through a generic discussion on strategy development, we can now turn our attention to how these concepts are, or are not, being applied to the development of strategies surrounding CIP. Acknowledging the Strategy Formulation model, this development should begin with a review of the NSS itself. Given the construct of that "grand strategy," it should be apparent that its objectives should serve as the first litmus test for a subordinate strategy's objectives (including its "immediate" implementing strategy, the NSHS), and that any path that will divert us from its objectives is a path that should be avoided.

Strategies for protecting the infrastructure should be in consonance with and extensions of the guidance provided by these two senior strategies. They should be either implementing strategies in their own right or supporting strategies for the same. Accordingly, strategic guidance for CIP will be drawn from the NSS, as supported by the NSHS, through the implementing strategies contained in the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets and the National Strategy to Secure Cyberspace. (See figure 7).

As pointed out earlier, the NSS reaffirms three national values: political and economic freedom, peaceful relations with other states, and a respect for human dignity. These, of course, are the ultimate "ends" to be pursued and protected by every aspect of our national power. The strategy then delineates eight "ways" to promote those values:

- Championing aspirations for human dignity
- Strengthening alliances to defeat global terrorism and working to prevent attacks against us and our friends
- Working with others to defuse regional conflicts
- Preventing our enemies from threatening us, our allies, or our friends with Weapons of Mass Destruction

Figure 7: Strategic Guidance for Critical Infrastructure Protection

- Igniting a new era of global economic growth through free markets and free trade
- Expanding the circle of development by opening societies and building the infrastructure of democracy
- Developing agendas for cooperative actions with other main centers of global power
- Transforming America's national security institutions to meet the opportunities and challenges of the 21st Century

The preponderance of the document is devoted to addressing how the resources of the United States could be applied through these "ways" to achieve those "ends" defined in our National Values, from the perspective of both domestic and international agendas.

The NSS's concerns over the importance of developing cooperative agendas for opening and securing world markets and free trade; for transforming America's security institutions to meet the new century's challenges and opportunities at home and abroad; and above all, for deterring and defending against global terrorism and weapons of mass

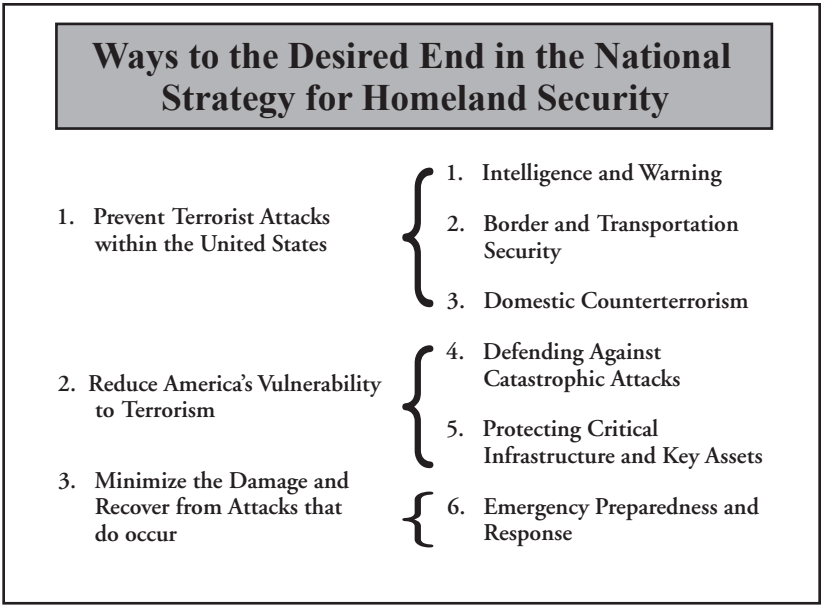

Figure 8: Ways to the Desired End in the National Strategy for Homeland Security

destruction, all find fertile ground for development in the NSHS, published in July of 2002. The NSHS is constructed upon three strategic objectives:

- To prevent terrorist attacks within the United States
- To reduce America's vulnerabilities to those attacks
- To minimize the damage and recover from attacks that do occur

The "external components" of our formulation model are of particular concern in this strategy as it attaches special emphasis in preventing, protecting against, and preparing for catastrophic threats, especially as those threats emanate from abroad. Concurrently, it outlines the ways and means for the Federal government to work with State and local governments and within the private sector to identify and protect our critical infrastructure and key assets.

The strategic concepts behind the homeland security strategy (or the "ways" toward its desired ends) are defined by the document's six critical mission areas:

1. Intelligence and Warning
2. Border and Transportation Security
3. Domestic Counterterrorism
4. Defending Against Catastrophic Threats
5. Protecting Critical Infrastructure and Key Assets
6. Emergency Preparedness and Response

The relationship between these mission areas and the strategy's objectives is immediately clear, as illustrated in figure 8.

But between these strategic objectives and the concepts to achieve them, the NSHS lays out a list of eight "principles."

1. Require responsibility and accountability–*focus on producing results through a clear delineation of requirements and authority*
2. Mobilize our entire society–*reinforce the position that homeland security is a national responsibility to be shared by Federal, State and local governments, and the private sector*
3. Manage risk and allocate resources judiciously–*identify, prioritize, and protect those assets that are most critical to the vital interests of the Nation in full knowledge that everything cannot be protected all of the time*
4. Seek opportunity out of adversity–*translate initiatives designed to enhance domestic security to concurrently advance other important public purposes*
5. Foster flexibility–*allow for the reassessment of priorities and the realignment of resources as the threat demands and response will allow*
6. Measure preparedness–*in keeping with the demand for accountability, identify benchmarks and performance measures for readiness*
7. Sustain efforts over the long term–*acknowledge that terrorism looms as a permanent specter over our people, and our initiatives will have to be measured over decades, not days*

8. Constrain government spending–*money spent does not translate directly to security; the safety of our citizenry will also be facilitated through government reorganization, legal reform, cooperative initiatives with the private sector, cost–sharing initiatives with State and local government, and the organized involvement of that citizenry*

These principles present something of a dilemma, in that they may not seem to fit neatly in an "ends, ways, and means" construct. However, closer examination may show that these are, in fact, a framework for the assignment and regulation of "means" to be devoted to our strategic ends. Expanding our resource base, measuring and demanding accountability for its expenditure, maximizing its utility through initiatives for dual benefits beyond domestic preparedness, and acknowledging the requirement for reappraisal of resources in response to a changing threat, are all reflective of a strategy keenly cognizant of the limits and values of its available means. Moreover, these principles are reflected in the NSHS's implementing strategies, including those associated with CIP.

Returning to the NSHS Critical Mission Area of "Protecting Critical Infrastructure and Key Assets," we are presented a perfect example of a strategic concept (way) in a senior strategy becoming a strategic objective (end) in a "follow-on" implementation strategy. Consider the eight "major initiatives" called for in the NSHS to promote CIP:

1. Unify American infrastructure protection efforts under DHS
2. Build and maintain a complete and accurate assessment of critical infrastructure and key assets
3. Enable effective State and local government and private sector partnerships
4. Develop a National Infrastructure Protection Plan (NIPP)
5. Secure Cyberspace
6. Harness the best analytical and modeling tools to build effective protective solutions
7. Guard America's Critical Infrastructure and Key Assets against "Insider Threats"

8. Partner with the international community to protect our transnational infrastructure

Balancing these initiatives against the strategic objectives of the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, we are faced with a good example of where the strategic concepts of a senior document (the NSHS) serve to define the strategic ends of an implementing strategy.

Similarly, it is not at all surprising to find clear commonality between senior strategy documents' strategic objectives and those of their supporting strategies. No better example can be found than in comparing the "desired ends" of the NSHS and the National Strategy to Secure Cyberspace (See figure 9).

This brand of commonality is… or should be… a consistent theme in the strategies that define our National Security institutions. If the NSS calls for the development of "cooperative agendas with other centers of global power," it is altogether proper that the NSHS should pursue partnerships "with the international community to protect our transnational infrastructure." If a major initiative of the NSHS calls for "enabling effective partnership with State and local governments and the private sector," the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets is clearly on the mark in pursuing a strategic objective assuring "infrastructure protection by enabling a collaborative environment in which Federal, State, and local governments and the private sector can better protect the infrastructures and assets they control." And when the President of the United States lists "responsibility and accountability" as the first principle of the NSHS, it should not be surprising to find sector-specific responsibilities deliberately assigned in the national strategy for critical infrastructure and key asset protection.

The point to be made here goes well beyond format. There is a continuity of direction and purpose that should be displayed in our strategies that will be essential not only in terms of efficiencies, but equally in terms of effectiveness. That continuity follows a steady azimuth from a foundational commitment to this Nation's values through the national interests and national objectives required to promote and protect them. It is committed to a judicious husbanding of resources that will always be constrained, but devoted to devising a concept of employment that

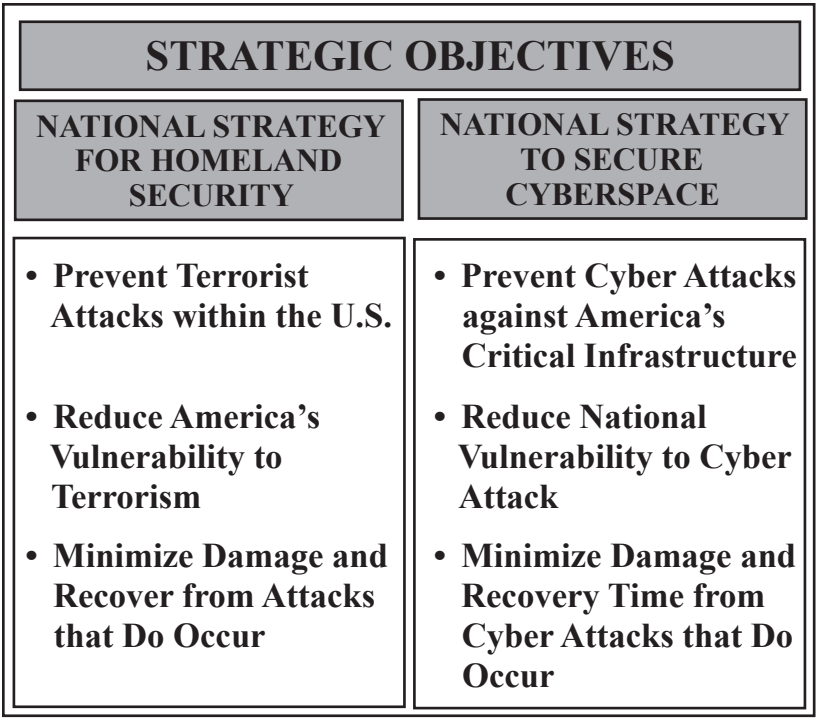

Figure 9: Strategic Objectives

will see those means fulfill their required end. It will remain flexible and adaptable, but always accountable. And it will succeed in directing a concerted national effort of our government, our people, and our livelihood in support of the common defense.


Prudens
Futuri

ENHANCING CRITICAL INFRASTRUCTURE PROTECTION (CIP)

Results of the U.S. Army War College Senior Symposium, 25 May 2004

Dr. Kent Hughes Butts

National Security Issues Branch
Center for Strategic Leadership
U.S. Army War College

In the *National Strategy for Homeland Security* (NSHS), President Bush identified protecting critical infrastructure and key assets as one of the strategy's critical mission areas. Clearly vital in its importance as a national security interest of the United States, this mission requires "protecting the assets, systems, and functions vital to our national security, governance, public health and safety, economy, and national morale," and, in so doing, "denying terrorists the opportunity to inflict lasting harm on the United States."[1] In support of this mission, the Center for Strategic Leadership of the United States Army War College conducted a Senior Symposium on 25 May 2004 at the Collins Center, Carlisle Barracks, Pennsylvania. The forum consisted of a distinguished panel of retired general officers and senior civilians from both the public and private sectors. The participants were intimately involved in numerous homeland security initiatives, and each had experience in dealing with questions associated with critical infrastructure and key resource protection. The diversity of their responsibilities and experiences allowed for an informed and probing analysis of the current state of the CIP process, the identification of shortfalls therein, and recommendations for addressing the same. The symposium would eventually focus on three areas: the identification and prioritization of CIP, approaches to

[1] The White House, *The National Strategy for Homeland Security*, (Executive Summary), Washington D.C., July 2002, p. ix.

forming partnerships between the public and private sector in addressing CIP, and the role of the National Guard in CIP efforts.

Critical Infrastructure Protection

The protection of the United States' critical infrastructure is an imposing task. Citizens of the U.S. have come to expect reliability in the provision of services and goods from all of the thirteen critical infrastructure sectors identified in the NSHS.[2] Other than labor strike disruptions, the chief threat to U.S. critical infrastructure prior to 9/11 had come from man-made accidents or natural disasters. Events such as the incident at Three Mile Island and Hurricane Andrew have generally been widely spaced, isolated geographically and temporally, and limited in the number of fatalities that they have generated. The September 11 attacks on the World Trade Towers, however, raised the public awareness of a more insidious and potentially much more deadly threat.

Although some would refer to the critical infrastructures of the United States as robust and resilient, the sectors are varied, each containing thousands of assets, and relatively vulnerable to a concerted attack by well-trained and financed operatives. The sheer volume of American critical infrastructure should be humbling for those responsible for its protection. There are, for example, 300,000 oil and natural gas production sites, 2 million miles of pipelines, and 2,800 electrical power plants to protect. Of these, 104 are nuclear power plants. In the area of water resources the U.S. has 1,800 Federal reservoirs, 1,600 municipal wastewater facilities, and 80,000 dams. In other sectors, there are nearly 2 million farms, 2 million miles of telecommunications cable, 137 million postal and shipping delivery sites, and 66,000 chemical plants. Protecting these and the airports, railroads, seaports, mass transit facilities, government facilities, hospitals, and so much more that falls under our definition of "critical infrastructure" is a complex mission that will involve the combined strengths of the Federal, State, local, and private sectors.[3]

---

[2] Ibid., p 30. The thirteen critical infrastructure sectors are: Agriculture; Food; Water; Public Health; Emergency Services; Government; Defense Industrial Base; Information and Telecommunications; Energy; Transportation; Banking and Finance; Chemical Industry and Hazardous Materials; and Postal and Shipping.

[3] The White House, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (NSPPCI), Washington, D.C., February 2003, p. 9.

The Complex Equation

In an attempt to begin framing their discussion, several members of the panel pointed to the chemical industry as a compelling example of the complexity of and political difficulties associated with protecting critical infrastructures and key resources. Chemical plants use a variety of materials, from petrochemicals and industrial gases to basic organic chemicals, plastics, and resins. Similarly, other industries require substantial "feedstocks" of chemicals to produce pesticides and fertilizers and to refine other products.[4] At the same time, the value of the chemical sector to the U.S. economy cannot be overstated. Commodities ranging from agricultural fertilizers to plastics polymers, providing services ranging from petroleum refinement to the healthcare industry, consume nearly $100 billion of chemical sector products. Ten percent of U.S. exports come from the chemical sector, making it the country's leading export industry. Moreover, nearly fifteen percent of all U.S. patents are granted to the chemical sector. The industry itself varies markedly in size and products. It is highly competitive, proprietary in nature, and depends upon public and consumer confidence for its vitality. The variety of products, technology, and chemical processes taking place in the thousands of chemical facilities around the U.S. makes security an expensive endeavor, and the complexities surrounding the issue defy any attempts to establish a single security regime for the entire industry.[5]

The U.S. government has identified 140 toxic or flammable chemicals that represent "the highest risk to man and the environment."[6] There are 15,000 chemical and other industry facilities that store, use, or produce potentially harmful quantities of these chemicals. In a post 9-11 study, the Environmental Protection Agency (EPA) found that 123 U.S. chemical facilities have worst-case, chemical release scenarios in which over one million people could be exposed to a toxic chemical release. In addition, another 700 facilities have the potential to threaten 100,000 people, and 3,000 other facilities have the potential to expose at least

[4] Government Accounting Office, *Homeland Security, Voluntary Initiatives Are under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown*, GAO-03-439, Washington, D.C., March 2003, p. 3.

[5] NSPPCI, February 2003, p. 65-66.

[6] Government Accounting Office, March 2003, p. 5

10,000 people to potentially fatal levels of chemical gases.[7] In October 2001, then Army Surgeon General, LTG James B. Peake, estimated that terrorists attacking a large chemical plant in a heavily populated urban area could force approximately 2.4 million people to seek medical attention.[8]

The Agency for Toxic Substances and Disease Registry in the U.S. Department of Health and Human Services stated in a 1999 report that "security at chemical plants ranged from fair to very poor," and pointed out the value of chemicals to recent terrorist attacks and the potential threat they held for the future.[9] In spite of this foreboding portrayal, a comprehensive assessment of chemical plants' security has yet to be accomplished.

The question of how to protect the chemical sector has been and continues to be heavily debated. The chemical industry believes that voluntary industry actions are sufficient; others, to include the Administrator of the EPA and the Secretary of Homeland Security, believe that "the federal government should impose security requirements on chemical facilities."[10] Process, safety, and transport in the chemical industry are regulated by multiple Federal laws and regulations aimed at protecting human health and the environment. However, these aged guidelines are not designed to deal with the terrorist threat; "there is currently no clear, unambiguous legal or regulatory authority at the Federal level to help ensure comprehensive, uniform security standards for chemical facilities."[11] The *National Strategy For The Physical Protection Of Critical Infrastructures And Key Assets*, signed by President Bush in February of 2003, directs the DHS and the EPA to work with the Congress to develop and pass legislation requiring chemical plants having high volumes of hazardous chemicals and located near heavily populated

[7] Ibid

[8] U.S. Army, Draft *Medical NBC Hazard Analysis of Chemical-Biological-Radiological-Nuclear-high Explosive Threat, Possible Scenarios & Planning Requirements*, Army Office of the Surgeon General, Washington, D.C., October, 2001.

[9] Common Cause, "Chemical Reaction: Despite Terrorism Threat, Chemical Industry Succeeds In Blocking Federal Security Regulations," Press Release, January 27, 2003, <http://www.mapcruzin.com/news/terrorspeak012803a.htm>.

[10] Government Accounting Office, March 2003, p. 2.

[11] NSPPCI, February 2003, p. 65.

areas to "undertake vulnerability assessments" and "take reasonable steps to reduce the vulnerabilities identified."[12]

The chemical industry has undertaken a number of voluntary activities to address the security issue. The American Chemistry Council is requiring its members to assess security vulnerabilities and, where shortfalls exist, to take corrective actions. However this group represents only seven percent of the 15,000 chemical plants subject to the Clean Air Act risk management requirements. Security initiatives are being developed by other chemical industry organizations; however, they vary in scope and the degree to which they require vulnerability assessments. A single, industry-wide organization that could ensure industry security standards does not exist in the chemical sector. As a result, "a significant percentage of companies that operate major hazardous chemical facilities do not abide by voluntary security codes developed by other parts of the industry."[13]

The chemical industry has been able to discourage the enactment of congressional legislation directing it to assess vulnerabilities, implement prevention in response plans, and (if necessary) change production methods.[14] It remains to be seen whether the EPA and DHS will be successful in encouraging Congress to enact the legislation sought by the White House. However, the chemical industry has successfully gained the support of some local and state emergency response officials, who believe that it is making sufficient progress in the area of security against terrorist attacks.

The case of the chemical industry illustrates the difficulty of dealing with CIP in the United States. Chemical industry facilities are usually located within municipalities. Not only must the chemical industry work with local authority and respond to municipal regulations, they must also abide by state and, as regards the EPA, regional approaches. At the national level, eight designated agencies outside of DHS affect chemical industry equities; much work remains to be done in coordinating their CIP programs. In findings from its well-received *Silent Vector* exercise,

[12] Ibid, p. 66.

[13] Ibid, p. 66

[14] Common Cause, January 27, 2003. <http://www.mapcruzin.com/news/terrorspeak012803a.htm>.

the Center for Strategic and International Studies (CSIS) said that, "it is chemical facilities that posed the greatest vulnerability and need to be fortified to safeguard against terrorist attacks." In the exercise's after action report, CSIS takes the Federal government to task for failing "to specify the roles and responsibilities of each Federal agency partnering with the chemical industry," and calls for the development of "appropriate information sharing mechanisms."[15] While the administration has taken the lead in drafting multiple strategies and policies for dealing with homeland security, Congress has much to say about the actual legislation and budget authority of the various agencies. Eighty-eight congressional committees and subcommittees have some form of authority over aspects of "homeland security." Such a spread of oversight authority challenges not only DHS but also the private sector and its various industry organizations in paying homage to these congressional bodies.

Prioritization of Critical Infrastructure Protection

The panel held that the multiple strategies and documents that address CIP in the post 9/11 environment are strong on generalities and the identification of Lead Federal Agencies; however, to date, they have failed to prioritize the large and intimidating list of critical U.S. infrastructure and key resources. If everything is a priority, then nothing is a priority. Without specifying priority assets within the critical infrastructure sectors and without designating prevention and response processes and organizations to attend to those assets, the public and private sectors will not be able to achieve efficiencies required in CIP.

This lack of specificity, the forum suggested, is a result of three things. First, the bureaucracies associated with all four sectors (Federal, State, and local governments, and the private sector) are substantial, and the decision to create a new lead agency, DHS, to direct the CIP process has created the inevitable startup opportunity costs. Some key positions at DHS remain to be filled and working relationships with other Federal agencies, as well as state, local, and private sectors take time to develop. Second, unlike traditional national security

[15] Center for Strategic and International Studies (CSIS), *CHEMICAL FACILITIES VULNERABLE: Operations Present Control Problems; Alert System Must Be Improved*, Washington, D.C., CSIS, December 23, 2003.

problems that depend upon the Federal elements of power for the development and execution of strategies, the problem of protecting critical infrastructure and key assets is largely a local problem to be solved by local, state, and private entities—with the *support* of the Federal government. Third, the sensitive issue of states' rights and the current political correctness reflected in the reduction of the size of the Federal footprint have further complicated the issue. Thus, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* clearly identifies lead Federal departments and agencies for CIP but only charges them with the responsibility for "coordinating protection activities and cultivating long-term collaborative relationships with their sector counterparts." They are to assist State and local governments and private sector partners as they attempt to organize protection and continuity of operations planning, identify and promote risk management and protection planning, and expand voluntary information sharing among the sectors.[16]

The panel was unanimous in their position that solutions to the prioritization dilemma surrounding CIP should begin at the top, but that the current structure for leading that prioritization was not up to the task. The organization for homeland security at the Federal level is awkward and unnecessarily bureaucratic. The DHS is composed of twenty-two agencies that are not collocated. Compounding this difficulty is the problem of managing the other seven agencies with CIP responsibilities by retaining a Homeland Security Council (HSC). The panel contended that the President should move homeland security concerns back under the National Security Council (NSC), which has the Executive Branch's greatest experience in orchestrating deputies' meetings and interagency programs, and thereby lend weight to homeland security's designation as "the Nation's top national security priority." A separate HSC is another layer of bureaucracy, stood alongside the NSC. It risks competition with that proven, "senior" council that could result in a tragic and unnecessary clash of agendas. The panel was of the opinion that the best means of ensuring that homeland security is our first priority was by examining it as the foundational component of all national security issues. By extension,

[16] NSPPCI, February 2003, p.17.

this streamlined homeland security architecture would be the first step in providing strong national leadership in CIP.

Identifying, assessing, and prioritizing critical infrastructure and key assets is essential to protecting CIP. PDDs 63 and 67 dictated that a critical infrastructure vulnerability assessment be conducted and a list of minimum essential assets for each infrastructure sector be compiled. The panel pointed out that neither of these requirements has been accomplished.[17] Without a prioritization it is not possible to determine what resources are necessary to protect critical infrastructure. The forum conceded that prioritization is a painful, however necessary, process that will almost certainly lead to friction between the private and the public sectors, across Federal, State, and local governments. Nevertheless, they pointed out that, without this hard prioritization, the country would be unable to discern those assets that the United States *needs* to protect versus those that the country might instinctively *want* to protect.

One of the panel members observed that there is currently no clear understanding of the activities that must be accomplished to protect CIP, or desired standards for their conduct. He suggested that, to bring clarity to the requirements and responsibilities surrounding them, DHS should develop "fifteen most likely CIP-related scenarios" and create a Mission Essential Task List (METL) for Federal, State, local, and private sector authorities to address them. The Federal government could clearly identify its areas of responsibility and suggest areas of responsibility for the other three sectors. Those sectors, in turn, could identify gaps in their response capacities, initiate training programs to fill the gaps, and otherwise request specific Federal support. A secondary objective in developing these scenarios would be to develop common standards for CIP that could be applied to strategic (national), operational (regional), and tactical (state, local, private sector) levels.

The Government and the Private Sector

In March of this year, Senator Byrd of West Virginia declared**,**

> …there is no mandate on the private sector to make these security investments. The private sector's involvement is completely

[17] The White House, *PDD-NSC-63, Critical Infrastructure Protection*, Washington, D.C., May 22, 1998.

> voluntary. There are no benchmarks in place to assess the private sector's role in critical infrastructure protection.[18]

There was a clear understanding among the symposium's participants that the relationship between government and the private sector in CIP is complex and problematic. Likewise, there was no question over the essential nature of the partnership between the two. One participant pointed out that, according to Admiral James Loy, former Commandant of the Coast Guard and currently the Deputy Secretary of the Department of Homeland Security, the operation and ownership of up to 85 percent of U.S. critical infrastructure is in the hands of the private sector, and therefore, beyond the direct control of the Federal government.[19] The approach of the Bush administration is that, "the private sector remains the first line of defense for its own facilities."[20] As Admiral Loy explained to a group of industry representatives in Washington D.C., "You are in the best position to tell us where your vulnerabilities lie….and how we can help in the process."[21] The Federal government is depending upon private sector owners and operators to examine the current terrorist threat, conduct risk assessments that reflect this threat, and modify their security planning, operations, and investment programs to reflect these assessments. As the case of the chemical industry demonstrates, this approach is providing mixed results. This led the symposium's members to ask openly, "How can this process be enhanced?"

The roles and responsibilities of the private sector and Federal government in CIP are laid out most clearly in the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* and can best be described as a partnership. Private industry is highly competitive, oftentimes with narrow profit margins as its main focal point. Investment in security affects profit margins and must be made in accordance with a "risk versus trade-offs" mentality. Industry leaders will, therefore, first seek to determine the potential risk to their infrastructure. Following

---

[18] Byrd, Robert C., Press Release, Sen. Byrd Calls For Investigation on Security Critical Infrastructure, Washington, D.C., March 2, 2004.

[19] Strohm, Chris. "Homeland Security Looks To Industry To Secure Nations Infrastructure." Government Executive, January 12, 2004.

[20] NSPPCI, February 2003, p.20.

[21] Strohm, Chris, January 12, 2004.

that assessment, they will determine what investment in security is economically justifiable in a resource-scarce environment. This current reality led several panelists to insist that the Federal government must lead cooperative efforts between the public and private sectors by providing timely and relevant risk information on which these decisions may be made. It should also provide access to best practices, support to industry when reasonable investment in security is insufficient to meet the threat, and "provide consistent guidance and criteria for sector specific protection planning and investment."[22]

Several members of the forum commented on areas in which this partnership can be improved, but generally the needs centered around leadership, standards, and incentives. As described above, a prioritization of critical infrastructure and key assets needs to be completed so that an assessment of vulnerabilities can be completed, thus providing an informed basis upon which to target Federal support to the private sector. The vulnerability assessment program needs standards so that it is possible to compare the vulnerability of the electric power industry in California with that of Virginia. The current process lacks discipline and consistency. The government would then have a prioritized plan that could be used as a basis for allocating resources to the most critical private sector industries. As the Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) has demonstrated, with regard to the chemical industry, standards change behavior.[23] The Federal government should impose mandatory standards and provide resources, but, in most cases, should allow regional and state regulators to manage compliance with the private sector.

The participants noted that there are other areas where the private sector-governmental partnership may be improved. Recognizing that the private sector has a competitive advantage that it must protect while meeting the demands of Federal regulation, they suggested that the government continue its efforts to create incentive options to encourage private sector investment in security. Grants, tax codes, and the insurance industry offer viable incentive alternatives. Information Sharing Analysis

[22] NSPPCI, February 2003, P. 20.

[23]United States Environmental Protection Agency, *CERCLA Overview*, Washington, D.C., October 17, 1986, December 11, 1980.

Centers (ISACs) could be improved by enhancing the public-private interface. This interface could help in clarifying issues like the terror alert levels issued by DHS. These alert levels can result in significant expenditures for the private sector, which is, therefore, reluctant to react to them without a clear explanation from the Federal government.

Members of the symposium were of a common mind in their belief that prioritizing and assessing CIP targets will create requirements for information sharing between the public and the private sector. Creating secure and efficient processes for sharing this information, therefore, should become a top priority, even if it requires additional legislation. Along a similar vein, the participants suggested that the Federal government might encourage the acquisition of secure communications systems that would allow access and interoperability between the three levels of government and private sector organizations. Likewise, the Federal government should encourage private and public sectors to share their risk management models, seeking best practices and valuable synergies. And returning to concerns over the particular responsibilities of the private sector, one participant suggested the promulgation of legislation aimed at delegating "CEO accountability" for reasonable efforts to provide for the security of their companies. The Sarbanes-Oxley Act of 2002 establishing financial accountability could provide a framework for this legislation.[24]

The Role of the National Guard

The *National Security Strategy of United States* (NSS) identifies Homeland Security as the Nation's first priority. The *National Military Strategy* (NMS) reiterates that position, stating that "the armed forces employ military capabilities at home to protect the Nation, the domestic population and critical infrastructure from direct attack."[25] The NMS goes on to include language supporting and clarifying the role of the military in homeland defense and CIP. The role of the armed forces in homeland security is multilayered and emphasizes a contention that the

[24]Securities and Exchange Commission, Division of Corporation Finance: Sarbanes-Oxley Act of 2002 – Frequently Asked Questions, Washington D.C., November 8th and 14th, 2002.

[25] The Joint Chiefs of Staff, *The National Military Strategy of the United States of America (Draft),* (Washington, DC: U.S. Joint Chiefs of Staff, 2004), p. 2

military's first line of defense against terrorist attacks is overseas. However, Department of Defense forces have responsibilities at home that include critical infrastructure protection, supporting law enforcement agencies for special events, and supporting civil authority in consequence management following attacks or when catastrophic events exceed their capabilities.[26]

It was the opinion of the participants that the National Guard should be seen as the DoD's first line of response in addressing critical infrastructure protection. The Guard's direct responsibility to the governors of their respective states, their traditional use in supporting civil authorities in response to natural disasters, and their "core capabilities" resident in engineer, medical, transportation, and aviation units all recommend the National Guard as "forward deployed" forces for the CIP mission. In addition, the National Guard has access to a wide variety of civilian capabilities through its "citizen soldiers" who are already being used creatively in some locales to support efforts to protect critical infrastructure from terrorist attacks. A recent example of the same was played out by the California National Guard which, working with the California Office of Criminal Justice Planning and of the California Antiterrorist Information Center, prioritized the state's critical assets according to potential vulnerability to terrorist attacks.[27]

The panelists went on to assert that there are several areas where the National Guard's contributions to CIP could be improved and expanded. The newly established Full Spectrum Integrated Vulnerability Assessment (FSIVA) initiative being exercised by some elements of the Guard is a program worthy of emulation that could provide an immediate service to Federal, State, and local identification and prioritization efforts surrounding critical infrastructure and key resources. In structuring and equipping the Guard for the Homeland Security mission, panel members suggested that we step back from Cold War attempts to "mirror image" the active component and assume a posture better configured to meet the terrorist threat. At the same time, they voiced concerns over the effect of long-term mobilization of the Guard for service in Iraq and the overseas

[26] Ibid, 2004, P. 9.

[27] Using the U. S. military's CARVER methodology (Criticality, Accessibility, Recuperability, Vulnerability, Effect, and Recognizability), the team identified, assessed individually, and rank ordered six hundred sites.

war on terror, questioning how this might eventually impact what they felt should be the primary role of "providing rear area security for the states." Finally, the forum noted that a significant number of local and state first responders are also members of the National Guard. This fact, they suggested, combined with continued extended deployments, could eventually cause state governors to lobby for limitations on the overseas commitments of the Guard.

The United States Northern Command's (NORTHCOM) dual mission of supporting homeland defense and providing military assistance to civil authority clearly recommends it as part of the solution to the country's CIP concerns. As DOD CIP policy is being revised in response to HSPD-7, NORTHCOM expects its CIP mission will also be revised, perhaps to include a central role in coordinating prioritization and protection efforts with the National Guard.[28] The symposium's members believed that while NORTHCOM matures and as its role in CIP is clarified, there are several areas in which NORTHCOM's contributions should be examined. Chief among these should be training and exercise initiatives wherein NORTHCOM could make a significant contribution by expanding events with DHS, DOD Homeland Defense (HLD), the Joint Forces Command (JFCOM), the domestic U.S. Army headquarters (CONUSAs), and Guard headquarters in each of the individual states. Such training and simulation events would help clarify the roles of these various organizations in responding to CIP requirements and would establish needed coordination channels between them. In looking across the range of requirements that could accompany these new imperatives, however, some members of the panel suggested that consideration should be paid to combining NORTHCOM and JFCOM under the next Unified Command Plan. They contended that the current trend in developing CONOPS for domestic security without identifying units to train for and execute the mission may be a prelude to failure.

Conclusion

The Senior Symposium offered an opportunity for an informed group of senior leaders to review variables within the critical infrastructure and key assets protection process and make recommendations for

[28] United States Northern Command, *Strategic Plan For Critical Infrastructure Protection* (Draft), February 18, 2004, p.14.

improvements. Several overarching themes emerged that underpin their recommendations.

- The U.S. government should provide leadership, standards, incentives, and resources to support the CIP process, but should delegate the "management mission" to state, local, and private sectors.
- Homeland security in general, and the CIP process in particular, needs strong leadership in Washington D.C.—including revamped, focused congressional oversight—in order to accomplish their strategic objectives.
- Success in virtually all areas of the CIP process requires a baseline vulnerability assessment and prioritization of possible infrastructure targets, as required first in the 1998 PDD-63, and reiterated in the recent HSPD-7. Several elements of the DoD may contribute toward this end, but the primary effort should be led by NORTHCOM and the National Guard.

Much goodwill and many successful efforts have characterized the work of those dealing with the trials surrounding CIP to date, but a great many challenges remain. The findings and recommendations of the distinguished panel brought together in Carlisle in May 2004 are indicative of the direction that must be taken in converting those challenges to solutions.

REFERENCES

Allison, Graham, *Preparing For Terrorism, Dirty Bomb*, NOVA Science Programming on Air and Online, TV Program, PBS, February 25, 2003.

Associated Press, *Fort Wayne based Guard unit to undergo anti-terrorism training*, Fort Wayne, IN, August 5, 2004.

Byrd, Robert C., Press Release*, Sen. Byrd Calls For Investigation on Security Critical Infrastructure*, Washington, D.C., March 2, 2004.

California National Guard Task Force, *Critical Assets in California*, California Anti-Terrorism Information Center (CATIC), February, 2003.

Center for Strategic and International Studies (CSIS), *CHEMICAL FACILITIES VULNERABLE: Operations Present Control Problems; Alert System Must Be Improved*, Washington, D.C., CSIS, December 23, 2003.

Central Intelligence Agency, DCI's Worldwide Threat Briefing, *The Worldwide Threat in 2003: Evolving Dangers in a Complex World*, Langley, VA, February 11, 2003.

Common Cause, "Chemical Reaction: Despite Terrorism Threat, Chemical Industry Succeeds In Blocking Federal Security Regulations," Press Release, January 27, 2003, < http://www.mapcruzin.com/news/terrorspeak012803a.htm >.

Department of Homeland Security, Nuclear Assessment Program, *Open Source Reporting: Illicit Trafficking of Nuclear Materials*, Washington, D.C., February 2003.

Department of Homeland Security, *Protecting The Homeland: Fiscal Year 2004 Budget,* Washington, D.C.

Doyle, John M., *U.S. Government Could Learn From Industry's Security*, Vol 3, No. 28 July 14, 2004, P. 4.

Government Accounting Office, *Homeland Security, Voluntary Initiatives Are under Way at Chemical Facilities, but the Extent of Security Preparedness Is Unknown*, GAO-03-439, Washington, D.C., March 2003.

Jackson, William, *DHS Struggles to Close Vulnerabilities in nation's infrastructure*, Government Computer News, April 15, 2004

Nordin, John S., *Technical Dialogue, A Dirty Bomb Example: Cesium 197*, PEAC, The First Response, ARISTATEK, Laramie, WY, March 17, 2003.

Pingree, Chellie, Akron Beacon Journal, *Security may not go hand in hand with secrecy*, July 5, 2004, 4X Edition.

Securities and Exchange Commission, *Division of Corporation Finance: Sarbanes-Oxley Act of 2002 – Frequently Asked Questions*, Washington D.C., November 8th and 14th, 2002.

Sherman, Jason, Defense News, *Pentagon Ponders Huge Security Boost For U.S. Military Infrastructure*, May 17, 2004.

Strohm, Chris. *"Homeland Security looks to industry to secure nations infrastructure."* Government Executive, January 12, 2004.

The White House, *Executive Order on Critical Infrastructure Protection*, Washington D.C., October 16, 2001.

The White House, *Homeland Security Presidential Directive/Hspd-7*, *Critical Infrastructure Identification, Prioritization, and Protection*, Washington, D.C., December 17, 2003.

The White House, *Critical Foundations Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection*, Washington, D.C., October 1997.

The White House, *Executive Order 12656, Assignment of Emergency Preparedness Responsibilities*, Washington D.C., November 18, 1988.

The White House, *National Military Strategy of the United States of America, 2004*, Washington, D.C., 2004.

The White House, National *Strategy To Combat Weapons of Mass Destruction*, Washington, D.C., December 2002.

The White House, *PDD-NSC-63, Critical Infrastructure Protection*, Washington, D.C., May 22, 1998.

The White House, *PDD-NSC-67, Enduring Constitutional Government and Continuity of Government Operations (U)*, Washington, D.C., October 21, 1998.

The White House, *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (NSPPCI), Washington, D.C., February 2003.

The White House, *The National Security Strategy For Homeland Security*, (Executive Summary), Washington D.C., July 2002.

The White House, *The National Strategy To Secure Cyberspace*, (Executive Summary), Washington, D.C., February 2003.

The White House, *The National Security Strategy of the United States*, Washington D.C., September 2002.

U.S. Army, *Draft Medical NBC Hazard Analysis of Chemical-Biological-Radiological-Nuclear-high Explosive Threat, Possible Scenarios& Planning Requirements*, Army Office of the Surgeon General, Washington, D.C., October, 2001.

United States Environmental Protection Agency, *CERCLA Overview*, Washington, D.C., October 17, 1986, December 11, 1980.

United States Northern Command, *Strategic Plan For Critical Infrastructure Protection* (Draft), February 18, 2004.

Washington Internet Daily, Volume 5, No. 78, *DHS Witnesses Tell House Panels that Critical Infrastructure Protection is Progressing*, Washington, D.C., April 22, 2004.

Yarger, H. Richard, *Towards A Theory of Strategy: Art Lykke and the Army War College Strategy Model*, Carlisle, PA, 1997.


Prudens
Futuri

Federal Policy Toward Critical Infrastructure Protection: a GAO Assessment

Michael Gilmore

Senior Information Technology Analyst
Government Accountability Office

We all rely on infrastructure every day in our personal lives: on electricity, transportation, chemical production, water and food distribution, and so on. We expect these services to "be there and functioning" on a routine basis. Critical infrastructure protection (CIP) is the national effort to make certain that this expectation of routine services is met for the key drivers of our Nation's economy and security. The role of the Government Accountability Office (GAO) is to measure how effective the government's efforts are in meeting the requirements set forth in Federal policy. This presentation will describe GAO's role in more detail, provide a definition of critical infrastructure, describe the current CIP policy, and delineate some of the challenges that have been identified in GAO work that must be addressed as the Nation continues to improve our capability to protect critical infrastructure.

The GAO is a legislative branch agency that serves Congress by evaluating programs and departments to determine their effectiveness and efficiency. Our efforts, of course, are directed primarily at the Federal government; but our studies for CIP also delve into the private sector, which voluntarily participates in our studies. For example, we recently did a study to evaluate the critical infrastructure protection efforts as related to the financial services sector.

In addition, GAO maintains a list of programs that are at a high risk for fraud, waste, and abuse, and those that face major challenges in terms of economy, efficiency, and effectiveness. The CIP program, along with information security, is on that high-risk list.

The question was raised, "Is there an accepted definition for critical infrastructure?" The answer is yes. Critical infrastructure is defined as, "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security,

Sector	Sector-Specific Agencies
Agriculture	Department of Agriculture
Banking and Finance	Department of the Treasury
Chemicals and Hazardous Materials	Department of Homeland Security
Defense Industrial Base	Department of Defense
Emergency Services	Department of Homeland Security
Energy	Department of Energy
Food	Department of Agriculture and Department of Health and Human Services
Government	Department of Homeland Security
Information Technology and Telecommunications	Department of Homeland Security
Postal and Shipping	Department of Homeland Security
Public Health and Healthcare	Department of Health and Human Services
Transportation	Department of Homeland Security
Drinking Water and Water Treatment Systems	Environmental Protection Agency

Figure 1: Infrastructure Sectors and Sector-Specific Agencies

national public health or safety, or any combination of those matters."[1] Critical Infrastructure Protection includes activities that identify critical infrastructure and key resources (CI/KR), assess vulnerabilities, prioritize CI/KR, and develop protective programs and measures, because these activities ultimately lead to the implementation of protective strategies to reduce vulnerability.

This is not just a Federal effort. It is also a private sector effort, because, as has been reported, 85 percent of the critical infrastructure in the United States is owned by the private sector. Accordingly, the protection of critical infrastructure must be a partnership between the Federal, State, local, and private sectors. In order to facilitate this partnership, the Federal government has identified thirteen infrastructure sectors.[2] For each sector, an agency has been designated the Sector-Specific Agency (SSA) to coordinate and lead the infrastructure protection efforts within the interagency, between State and local governments, and with the private sector. The sectors and their agencies are shown in the figure 1. In examining these sectors in terms of "protection," it is important to understand that none of them

[1] USA Patriot Act

[2] Editor's Note: In addition to these, the government has identified four key resource sectors: Government Facilities; Dams; Commercial Facilities; and Nuclear Reactors, Materials, and Waste. The sector-specific agency charged with all four is the Department of Homeland Security

are "independent;" there are, to the contrary, a lot of interdependencies between sectors that must be addressed in efforts to protect any one of them. Information technology and telecommunications, for instance, is a critical sector in its own right and in light of the fact that most (if not all) of the other infrastructures rely upon it.

Natural disasters will always be a concern, but—as we all know—there is a growing urgency associated with man-made threats to our infrastructure—both physical and cyber. This human threat is stretched across a variety of actors—criminals, pranksters, spies, saboteurs, and even users who simply make mistakes. And, of course, it includes terrorists threatening the infrastructure through both conventional means and through weapons of mass destruction (WMD). Of particular concern in this regard is the "insider threat," portending deliberate destruction from within organizations that either house or are dependent upon given sectors of critical infrastructure. In fact, based on the most recent statistics, insiders continue to be the most frequently identified threat to critical infrastructure. But whether the threat is inadvertent or deliberate, man-made or natural, from within or without, its potential damage is equally debilitating. Figure 2 is illustrative of the potential threat and of potential effects.

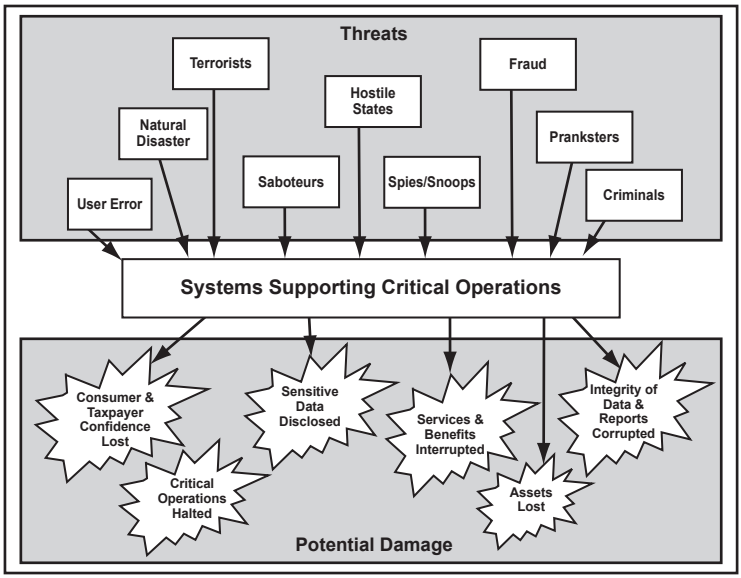

Figure 2: Potential Threats and Potential Damages to Systems Supporting Critical Operations

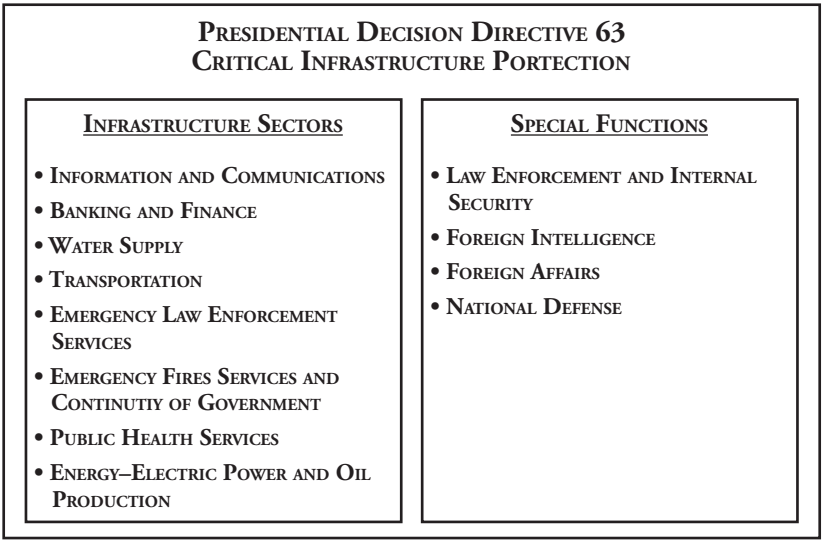

Figure 3: Infrastructure Sectors and Special Functions established in PDD-63

The Federal government's policies for critical infrastructure have developed through a series of documents. The first significant effort came with the President's Commission on Critical Infrastructure Protection's Report of October 1997, which focused on the country's increasing dependence on information and communications systems. It described the potentially devastating effects of poor information security for the Nation and recommended measures to achieve a higher level of CIP in the cyber realm.

Presidential Decision Directive 63 (PDD-63) of May 1998 attempted to implement the recommendation of the President's Commission's Report. It established CIP as a national goal and presented a strategy for cooperative efforts by government and the private sector. It specifically established government agencies to coordinate and support these efforts and identified lead Federal agencies, or sector liaisons, to work with coordinators in eight infrastructure sectors and five special functions (see figure 3). Finally, PDD-63 encouraged the development of Information Sharing Analysis Centers.

The *National Strategy for Homeland Security* (July 2002) identified the protection of critical assets and key resources as a critical mission,

and it expanded the number of infrastructure sectors to thirteen. The *National Strategy to Secure Cyberspace* (February 2003) provided an initial framework for both organizing and prioritizing efforts and set national goals for the protection of cyberspace. Finally, the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (February 2003) expressed the continuing commitment of the Federal government to protect critical infrastructure and key assets from physical attack

All of these documents identified priorities, actions, and responsibilities. However, some key elements are missing. For example, the separate cyber and the physical protection strategies do not sufficiently address the fact that the two environments are reliant on each other and that, consequently, the actions to protect one must be fully integrated with the actions to protect the other. They do not define the different roles, relationships, and responsibilities among the key players, including the State and local governments and the private sector. Finally, there are no timeframes or milestones for actually accomplishing anything; there are simply lists of all the things that we want to accomplish. That said, the DHS is in the process of taking the next major step in an evolving infrastructure protection strategy, through the mechanism of a National Infrastructure Protection Plan (NIPP). That plan, which will amount to an implementation of the aforementioned strategies, is designed to resolve some of these issues.

The Homeland Security Act (November 2002) is a crucial benchmark. It created the DHS and assigned it CIP responsibilities. To lead the CIP effort, the Information Analysis and Infrastructure Protection Directorate (IAIP) was created in DHS. In so doing, for the first time ever, this legislation established statutory responsibility for CIP activities.

Homeland Security Presidential Directive 7 (HSPD-7) of December 2003 both supersedes PDD-63, and provides direction for the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* and the *National Strategy to Secure Cyberspace*. It clarifies the actions required by the Homeland Security Act, and it defines responsibilities for DHS, SSAs, and other departments and agencies. It provides essential guidance for the interaction between these Federal agencies, State and local governments, and the private sector. From GAO's perspective, the

key aspect of HSPD-7 is that it requires and lays out metrics to measure performance.

The Secretary of Homeland Security is assigned a number of responsibilities under HSPD-7:

- Coordinating the national effort to enhance critical infrastructure protection
- Identifying, prioritizing, and coordinating the protection of critical infrastructure, emphasizing protection against catastrophic health effects or mass casualties
- Establishing uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors
- Serving as the focal point for security of cyberspace, including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for critical infrastructure information systems
- Developing a comprehensive and integrated national plan for critical infrastructure and key resources protection that outlines goals, objectives, milestones, and key initiatives

In addition, HSPD-7 assigned responsibilities to the SSAs. Many of these were extensions of the responsibilities first assigned under PDD-63:

- Collaborate with Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector
- Conduct or facilitate vulnerability assessments of the sector
- Encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources
- Identify, prioritize, and coordinate the protection of critical infrastructure and key resources
- Facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices

- Annually report on their efforts to identify, prioritize, and coordinate the protection of critical infrastructure and key resources in their respective sectors

From the audit perspective, specifying these responsibilities and, especially, requiring annual reporting create the conditions for more effective monitoring, ensure accountability, and provide a method to determine what progress is being made.

This kind of accountability is reflected in several aspects of the directive. By July 2004, all Federal agencies were to have developed and submitted to the Office of Management and Budget (OMB) plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. Those plans were to have addressed identification, prioritization, protection, and contingency planning for the protection of this infrastructure, and recovery and reconstitution plans for essential capabilities in the event of an attack. Perhaps most importantly, the directive reiterates the requirement of the Homeland Security Act of 2002 by obligating the Secretary of the Department of Homeland Security to produce a comprehensive, integrated plan for CI/KR protection by 17 December of 2004, outlining national goals, objectives, milestones and key initiatives.

Much progress has been made, following many efforts dating back to well before 2001. However, much remains to be done. From the GAO perspective we see four major challenges. First, a complete and coordinated national CIP plan needs to be developed. This is essential for defining the relationships among all CIP organizations to ensure that the approach is comprehensive and well coordinated. Elements of the plan should include: delineating roles and responsibilities of Federal and non-Federal entities, defining interim objectives and milestones, setting time frames for achieving objectives,; and establishing identifiable, achievable performance measures.

Next, at all levels, we must implement better information sharing measures surrounding threats and vulnerabilities. In achieving this end, we must begin by overcoming procedural and cultural obstacles within and between our institutions, and building relationships founded on trust. We must continue to identify and define the roles of various government

and private-sector entities and overcome barriers to information sharing. These barriers include sensitivity issues surrounding information/intelligence, legal limits on disclosure, and contractual and business limits on how and when information is disclosed. Establishing this climate of trust will not be easy; the business community may be called upon to accept some risks whenever they share information with the Federal government. At the same time, the Federal government must be willing to extend certain "incentives" to those cooperating businesses, and—if necessary—to "compensate for market failure"[3] when demonstrated good faith results in economic setbacks.[4] The bottom line here is that the Federal government has many tools for motivating the private sector, to include grants and incentives, as well as regulations. But nothing is automatic; a tax break incentive isn't much of an incentive to a group that doesn't pay taxes. I would suggest, therefore, that incentives might have to be tailored for different industries, much the same as we tailor their regulations.

As we recently reported, DHS currently lacks a plan that clearly describes how it will carry out its information-sharing responsibilities and relationships. It lacks policies and procedures to ensure effective coordination and sharing with the private sector through their associated Information Sharing and Analysis Centers (ISAC). It has even less "structure" for encouraging and facilitating the flow of vital information to the government (Federal, State, and local) <u>from</u> the private sector. All three issues must be addressed if the oft cited "information sharing" maladies of critical infrastructure protection are to be overcome.

Analysis and warning shortfalls—that is, identifying and disseminating intelligence on an imminent threat effectively and efficiently throughout the public and private sectors—is a challenge that we first identified in 2001 when the "responsibility" lay with the National Infrastructure Protection Center (NIPC) of the FBI. We noted then that they

[3] As per the "Guiding Principles" of *The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (p ix).

[4] The latest GAO report on certain sector Information Sharing and Analysis Centers (ISAC) reemphasizes these challenges. See *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors,* GAO-04-780 (July 9, 2004)

lacked a generally accepted methodology for analyzing strategic cyber-based threats. Additionally, there is a lack of industry-specific data on factors such as critical system components, known vulnerabilities, and interdependencies. Both of these failings must be addressed.

Any capabilities that we develop will need to address both physical and cyber security. Great progress has been made, but great challenges remain. It is vital that these challenges be met.

Critical Infrastructure Protection: No Room for Complacency[1]

The Honorable Paul H. McHale

Assistant Secretary of Defense for Homeland Defense

Current CIP in the United States is dangerously inadequate. Many of you in this room have worked very hard to advance the cause of real protection as it relates to domestic critical infrastructure, but there is absolutely no room for complacency. We are in the first inning of a nine-inning ball game when it comes to the effective protection of critical infrastructure—civilian infrastructure as well as defense critical infrastructure.

Let me place that CIP challenge in context. I have had the privilege of wearing a uniform for over thirty years. Throughout most of that time, I, like many of you, trained for possible conflict against the Soviet Union. Our training reflected the doctrine of combined arms warfare in a mechanized environment. We envisioned that it would take the collective capacity of a nation-state, like the Soviet Union, or a coalition of nation-states, like the Warsaw Pact, to fundamentally challenge the national security of the United States. So the warfighting capabilities that we developed over those five decades of the Cold War reflected the reality of the threat confronting us. We thought we might go to war against the Soviet Union and its allies, and we prepared to defeat that threat, were it to materialize on an actual battlefield.

That fundamental threat changed in many ways at the end of the twentieth century. Obviously, the Soviet Union disintegrated into a series of emerging nation states, and that immediate threat was diminished—although not eliminated. However, beyond the disappearance of that immediate threat, I would argue that there was a fundamental change in the character of war that took place during that same period. Some of us noticed, and some of us did not. The reality of that change was imposed brutally upon us on September 11, 2001. At the end of the twentieth

[1] This text is an edited version based on a transcription of Secretary McHale's remarks.

century and moving into the twenty-first century, it has become painfully clear that asymmetric threats—transnational terrorist groups—possess the destructive capacities that had, in the past, only been associated with nation states. Because of emerging technology—including WMD technology—small groups of transnational terrorists, even individuals, could possess the kind of destructive force that formerly required the collective resources of a country.

The attacks of September 11 were fundamentally conventional in character: heartbreaking, brutal, almost unbelievably barbaric, but fundamentally conventional in their methodology. Commercial airliners were converted into weapons platforms, and jet fuel, along with traumatic force, ultimately produced the deaths of over three thousand people. I would argue that that was not an aberration, but rather a reflection of certain characteristics of the human spirit, albeit the very worst. We have always had Adolph Hitlers and Osama bin Ladens throughout the course of history. The difference today is that they, and those who are aligned with them, can acquire a destructive force that is unprecedented. As bad as September 11 was, if that attack had involved WMD, the number of casualties could have been far worse. In my judgment, there is no doubt that those same organizations and, in some cases, those same individuals still seek to acquire such weapons, and if given the opportunity to acquire and employ them against the United States, they will.

Thus, after September 11 we recognized that, as the threat had changed, our defenses had to change. Most immediately the President, the American people, and the Congress recognized that we had to reorganize our defenses dramatically to deal with the asymmetric terrorist threat—specifically the imminent threat posed by Al Qaeda—while we simultaneously preserved our capability to defeat hostile nation states, because it is still a dangerous world. Not only are there terrorists, but there are also nation states emerging as potential peer competitors who—as has happened in the past—might challenge the United States. So we had to build upon our capacity to defeat hostile countries in order to achieve a defense that would be equally capable of defeating the known and emerging capabilities of transnational terrorist groups.

In consequence, we reorganized the Federal government; 170,000 employees from twenty-two agencies were brought together to create

the Department of Homeland Security (DHS), the most significant reorganization of our government since the 1940s. Within the Department of Defense (DoD), we also recognized the changing threat environment, and we addressed how we should reorganize to deal with this evolving transnational threat. It became immediately clear that we had to modify the Unified Command Plan (UCP) to create a new geographic combatant command, subject to which the combatant commander would be assigned, for the first time since the days of George Washington, the personal and institutional responsibility to physically defend the United States of America, the airspace of the United States, and the maritime and land approaches to our country.

To fulfill this requirement, we created the U.S. Northern Command, NORTHCOM. We gave this new combatant command two responsibilities. First, to defeat any attack upon the United States within the assigned area of responsibility, which is essentially the landmass of the United States, Canada, and Mexico, the airspace, and the maritime approaches. The U.S. Pacific Command (PACOM) also has substantial homeland defense responsibilities within the homeland regions of the PACOM area of responsibility. However, by virtue of where most of our population lives and the geographic location of most of our territory, the preponderance of the homeland defense responsibilities have been assigned to NORTHCOM.

In the second half of its mission statement, NORTHCOM has been assigned the responsibility to provide civil support to various entities within government, at both the national and State level, in the event that the capabilities of the state and of other Federal agencies are overwhelmed. Most typically, this mission would be executed in partnership with DHS. If civilian capabilities are overwhelmed and the President declares a major disaster under the Stafford Act, the DoD stands ready to assist the Lead Federal Agency to meet its assigned responsibilities. Unlike homeland defense, where DoD has the lead, for civil support DoD is in support of another Lead Federal Agency, normally the Federal Emergency Management Agency (FEMA).

We also created the job of the Assistant Secretary of Defense for Homeland Defense, the job I currently hold, with the statutory

responsibility for overall supervision of all homeland defense activities of DoD.

At the time, as we were accomplishing all of this, we did not articulate our plans and our progress very well. Yet we accomplished much, and in a very short time. We stood up NORTHCOM. We established certain capabilities within NORTHCOM; we started flying daily combat air patrols to protect the airspace over the United States in a manner that we had never done prior to September 11; we established quick reaction forces on the ground to provide the capability to respond to a foreign threat on our soil, a capability that did not exist before September 11; and the Secretary of Defense went to the Congress, and with the support of the members of the House and the Senate, in the National Defense Authorization Act of 2003, we stood up the office of the Assistant Secretary for Homeland Defense, manning it with the outstanding individuals with whom I have the privilege of working. In short, although we started doing all of these things to respond to the immediate operational requirement, we have now begun to assemble these capabilities in support of an overarching strategy.

As part of this strategy, we recognized that our defenses could not be passive; they could not be merely responsive. If we sit in place, building a Maginot line, transnational terrorists, most especially Al Qaeda, will conduct a thorough reconnaissance of our defensive capabilities, and our homeland defense capabilities in particular. They will discover the seams, the points of vulnerability, and they will exploit those points of vulnerability to execute a successful attack upon the United States of America. We can not be passive; we must be active in our homeland defense. We must have a continuous and layered presence that is designed not only to respond to an enemy attack, if we are fortunate enough to see one coming, but is also designed to identify and interdict emerging enemy threats before they can fully develop their capability to attack, rather than waiting passively for an attack to be launched. We must seize the operational initiative, and in certain areas, including CIP, we have begun to do so.

The 9/11 Commission recently reported out and emphasized the need for significant intelligence reform. In short, the Commission recognized that, on September 11, while we were engaged—though

perhaps we did not realize it—in a global war on terrorism, we were still functioning with an intelligence capability that was firmly rooted in the parochial competitions of the Cold War. Our intelligence capability had been overtaken by emerging events. We had an intelligence collection capability and an information sharing system that may well have been properly designed for our struggle against the Soviet Union, but which was wholly inadequate to the far more decentralized, flexible, and—in some ways—more challenging offensive capabilities of terrorists. So the 9/11 Commission concluded that, in order to achieve an intelligence capability adequate to meet the twenty-first century transnational terrorist threat, we need to significantly modify our existing structures. Their argument is that we need to establish a National Counter Terrorism Center and that we need a new National Intelligence Director. It is too soon to say how this will turn out, but within the next six months all of this will result in a vigorous intellectual engagement regarding the reform of our intelligence community.

Just as our operational capabilities, now assigned primarily to NORTHCOM for homeland defense, had to be substantially changed to deal with the twenty-first century transnational terrorist threat, just as our intelligence capabilities must be reviewed, wire-brushed, and reformed to make them operationally relevant to the twenty-first century transnational terrorist threat, so too we must rigorously review and, I believe, dramatically change our concept of CIP. In my judgment, that review has only begun; it is certainly not complete, and our current defensive capabilities for the protection of critical infrastructure in the United States are inadequate.

Many extremely capable people, including many of you here today, have been deeply engaged in the implementation of the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*. Many of you have spent a great deal of time reading, analyzing, and initially implementing elements of HSPD-7, signed by the President in December 2003. This includes work in the interagency and academic communities to ensure that our CIP activities will be in conformity with that document, with the national CIP strategy, and, most importantly, will produce an effective defense of our nation's critical infrastructure. But we have not done nearly enough.

We are not yet out of a Cold War mentality when it comes to protecting our critical infrastructure. We still speak in terms of civil engineering concepts: redundancy, systems analysis, single points of failure. All of that has value, but it is insufficient. Those are concepts of systematic analysis that were absolutely essential during the Cold War, when we viewed the Soviet threat and tried to envision how that threat might defeat critical infrastructure in an actual conflict. Typically our analysis was oriented toward the potential of a nuclear exchange and the resultant diminished capacity in terms of transportation, communications, power transmission, and other key sectors in the event of a major conflict with the Soviet Union.

It is not that we should forget the experience of the Cold War; rather, we must build upon that experience. Redundancy, single nodes of failure, backup communications pipelines—all that is still relevant, still necessary for dealing with those emerging peer competitors, certainly those who possess or seek to possess nuclear weapons. Today, however, while such an analysis is still valuable, it is no longer sufficient. We are still stuck in the jargon and culture of the nation-state threat, but we are in the middle of an asymmetric war with Al Qaeda, not a thermonuclear confrontation with the Soviet Union. For example, while we continue to focus on the civil engineering characteristics of some hardened site, what have we done over the last three years to frustrate the obvious concept of operations of Al Qaeda of conducting a thorough and detailed reconnaissance of any target before an attack? When we thought about Soviet reconnaissance during the Cold War, it was typically a counter intelligence operation conducted by civilian law enforcement organizations, normally the FBI, or, if overseas, by the CIA or other appropriate agencies. However, it has become clear since September 11 that Al Qaeda never launches a haphazard attack.

We continually receive credible reports of ongoing reconnaissance by Al Qaeda within the United States in order to identify and exploit vulnerabilities with regard to domestic targets. In recent published news accounts you may have seen some reports on what may have been recovered from various computers that were seized overseas. Those reconnaissance activities were reflected in the material produced by the

analysis of those computers. In fact, that information, which resulted in a targeted elevation of the Homeland Security Threat Advisory System for financial institutions in New York, New Jersey, and Washington, D.C., gave evidence of a very, very thorough reconnaissance of critical infrastructure, comparable to the kind of target data that we would be able to produce on a good day. Yet, when we think of critical infrastructure, we still tend to think in terms of civil engineering analysis. What have we done to incorporate into a twenty-first century CIP analysis a conscious defensive capability that is designed to frustrate an Al Qaeda reconnaissance activity? We did not do that during the Cold War, and I do not believe that we have thought much about it at this stage in the Global War on Terrorism.

Critical infrastructure protection has not risen to the challenge; we are still attempting to apply a Cold War template to an asymmetric terrorist threat. We are still doing business—with a sense of urgency and with passion and patriotism—but without the capability required to ensure that our critical infrastructure is not successfully attacked. In the past we have taken an "all hazards" approach to CIP. It was almost as if it made no difference whether the Soviet Union or a hurricane brought down that power line. While we would look at causation, the major issue revolved around questions such as: How do we react if that power line does go down? How do we ensure that it won't go down? How do we provide a redundant capability if it does go down? That approach is not adequate to deal with the asymmetric transnational terror threat.

Certainly, all hazards must be addressed, but now we have competent adversaries who are conducting detailed reconnaissance and planning to take down our critical infrastructure, and to do so in a way that will cause maximum loss of life. Have we really adjusted our CIP mentality to deal with that kind of asymmetric threat, or are we just building incrementally on our earlier experiences in the Cold War? I would argue it is the latter.

In short, when it comes to CIP, we have not fundamentally reconceived and reoriented our approaches to meet today's threat environment. Where should we go from here? I believe that the following are the key CIP issues.

What is the appropriate role of DoD in providing additional security within the borders of our own country? When I left the Congress, I went

back home and, among other things, taught a course on the Federalist Papers. I would encourage you to read Federalist 8, where Alexander Hamilton talks about the appropriate role of the military in providing domestic security. I knew that the founders of our Nation had some concerns about maintaining a large standing army, but I did not know much more than that until I read Federalist 8.[2] The concern was not that soldiers would impose a military culture on an unwilling civilian society at the point of a bayonet. The real concern was that, if we relied excessively on the military capabilities for domestic security, the American people would, out of necessity, embrace that protection. If only the military was perceived as being able to protect the American people, the American people would see the military as their saviors, and it would be, as Hamilton phrased it, a short step to the willing acceptance of the military as not just their saviors, but as their superiors. A dependence upon the military for physical security would, over time, alter the civilian character of our government. We recognize this as a threshold issue in dealing with CIP. We recognize that, while DoD has an important role to play in providing for the defense of our citizens and our infrastructure within the borders of our own country, we should not have the lead in that regard, and we do not. Under the Homeland Security Act of 2002, HSPD-7, and the national CIP strategy, DHS quite appropriately has the lead. So we have to determine what the appropriate subordinate and supporting roles are for the military consistent with the philosophical concerns raised in Federalist 8.

What are the CIP responsibilities assigned to NORTHCOM? How do those CIP responsibilities interact with NORTHCOM's recently assigned Anti-Terrorism/Force Protection (AT/FP) mission? When we talk about the physical protection of a base or other military installation, are we not also inherently talking about the protection of critical infrastructure at that base or installation? Since NORTHCOM has now been assigned the lead role in regard to AT/FP of bases and installations in the United States, to what degree should NORTHCOM possess situational awareness of critical infrastructure at those bases and installations? And to what extent should NORTHCOM plan for protection of critical infrastructure at those bases and installations? We

[2] A copy of Federalist 8 is included in Appendix A.

cannot separate security at the perimeter from the reality of critical infrastructure vulnerabilities inside the wire.

How does this effect NORTHCOM's contingency planning? We have active duty quick reaction forces that were created after September 11. These are active duty soldiers and Marines prepared to engage in land warfare on the soil of the United States in a warfighting mode, exempt from posse comitatus. This is not law enforcement; we are talking about engaging foreign threats on our own soil. We have not had to worry about that threat for about two centuries, when in 1814 the British marched on Washington, D.C. and burned the capitol of the United States. We were clearly engaged in warfighting activities on our own soil. For the next two centuries, two oceans protected the United States. No longer is that the case. Now we have to worry about foreign adversaries, who may or not be associated with nation-states, coming on to our soil to attack targets. So we have active units of the Army and Marine Corps on alert, prepared to defend those potential targets should the need arise. Those reaction forces were primarily created in order to achieve CIP. The issue becomes, when should NORTHCOM be lawfully empowered to deploy soldiers on our own soil to protect against an emerging Al Qaeda attack, and what kinds of potential targets should be defended by those soldiers and Marines? Certainly, we have the responsibility to protect defense critical infrastructure that is located aboard a military installation, but should we be prepared to deploy those forces to defend civilian-owned infrastructure that is essential to the DoD mission? Should we be prepared to physically defend the facilities of a contractor who is a sole-source provider of some critical commodity if those facilities are located in the civilian community?

What about infrastructure that is critical to the United States but is not critical to, or an inherent part of, the Defense Industrial Base (DIB)—for example, a nuclear power plant? If we have a credible threat to that plant, should we have contingency plans in place to defend those facilities on the ground? What are the legal constraints? What are the coordination requirements with the states? A governor would be extremely unhappy to learn that the Federal government had deployed active duty military formations to his state without his approval or even without prior considerations. What should NORTHCOM envision as potential mission requirements?

What is the operational role of the National Guard in providing protection of domestic critical infrastructure? There is an amendment currently before Congress that would re-write Title 32 so that, under command and control of a governor, but at DoD expense, the National Guard may be employed not only for training missions (as is the case today under Title 32), but for operational missions, most notably, CIP missions. How do we coordinate and deconflict the roles of the governor, the President, and the Secretary of Defense when it comes to the use of the National Guard in this manner? If the National Guard is going to be used to physically protect, for example, a Defense Logistics Agency (DLA) contractor, and if the targets identified by Al Qaeda are in close proximity to major population centers, what kind of doctrine needs to be developed for our forces charged with protecting such sites without unduly endangering the surrounding civilian community?

If we talk about defending critical infrastructure or protecting critical infrastructure, we must understand that we are talking about the use of force. How do we develop doctrine, training, and equipment that will minimize the potential inadvertent threat to our own surrounding civilian communities? One approach is to dramatically speed up the development of non-lethal weapons. Not only the blunt trauma non-lethal weapons—rubber projectiles, bean bags from shotguns and so on—but newer technology. I believe that we will need to develop, train, and equip with weapons that are unprecedented. Currently, the U.S. Marine Corps has the lead for the development non-lethal weapons for DoD, and they have developed a microwave beam. The maximum effective range of that beam is classified, but it is comparable to small arms fire. When that beam strikes a target, it produces a painful, though non-lethal, effect. Although effective against a point target, unlike a round of ammunition, this beam presents no threat to the surrounding civilian community. Nevertheless, there are substantial legal and public policy issues to be addressed. The beam raises the skin temperature to 130 degrees, but the pain ceases as soon as you step out of the path of the beam. To the best of our knowledge, there is no permanent effect.

We have emerging capabilities that can be used to more safely protect against a terrorist attack while not endangering the surrounding civilian community. However, there are clearly profound legislative discussions that need to take place—perhaps statutory revision—before we would

consider using such a weapon, even for the most humane of purposes, within the United States of America. Is this an appropriate role for the National Guard? I would argue that it is, but we must approach that issue cautiously, with full and open debate, with full exposure to the Congress and the American people of what we are planning to do and why.

If we are using the National Guard for CIP under Title 32, and DoD is paying for it, how much is it going to cost? We did this for the G8 summit at Sea Island, Georgia and at the Democratic and Republican National Conventions, and we propose to do it again. We must be careful to link their mission assignments to current their Title 10 mission essential tasks. In some cases, we will use them to augment appropriate law enforcement capabilities. This provides us with National Guard forces, not subject to posse comitatus, in Title 32 at DoD expense, preparing to engage lawfully in military missions in order to ensure security against a high-end terrorist threat. It cost about $15 million to do that for the G8 summit. As we use the Guard in this capacity, what are the financial implications for DoD?

These are emerging homeland defense missions for the Guard. They bring tremendous utility in terms of the relevance of the National Guard to homeland defense, specifically CIP missions. We hope that, in the future, if we have a credible Al Qaeda threat against, let's say power plants, we would not use our Title 10 quick reaction forces and we would not use our active duty soldiers and Marines. Instead, we should use the National Guard to provide physical security at those sites when the threat is credible—and certainly when the threat is credible and imminent. However, we are going to have to pay for this newly imposed requirement, imposed not as a matter of policy analysis, but as a result of the obvious threat. Al Qaeda wants to hit us in our own country; they want to do so by attacking critical infrastructure and simultaneously causing the maximum number of American casualties. The National Guard is well-suited and potentially can be well trained to protect against this very real threat. While there is operational utility in empowering the Guard to do so, there are costs associated. How expensive is it going to be to meet the expense of such National Guard deployments?

We need to better define the DIB. I know there are definitions in the various documents, but we are still not clear on what is really included in the DIB. Critical infrastructure aboard an installation? Yes, definitely. Defense contractors who provide a critical service? Yes, without question. But what about a nuclear power plant that provides essential electricity for a DoD installation and also provides power to an entire region of the country? Whose responsibility is it to protect that plant? What about a transportation corridor, a rail line between a post and a port of debarkation? Should NORTHCOM have contingency plans to protect that rail line from fort to port, or is that a civilian law enforcement responsibility? I would argue that it is law enforcement's job, primarily. Does the National Guard have a contingent mission to protect such infrastructure? I would argue yes. However, should NORTHCOM have contingency plans to protect such infrastructure? Does NORTHCOM have a duty under HSPD-7 to protect and to plan for the protection of a nuclear power plant that serves an entire region of the country, to include DoD installations within that region? Who is in charge? Whose duty is it to protect that power plant? In these areas, I do not believe that we have defined the issue very well. We all have some intuitive understanding of what is in the DIB, but the gray area is quite large. The degree of definition that we can give that gray area will determine the degree of detail that can be incorporated into NORTHCOM's contingency plans. We are not yet there, both in terms of defining what is in the DIB and in terms of NORTHCOM's contingency plans to ensure its protection.

Should we revise DLA contracts to impose much stronger security requirements upon private contractors? The first level of security at a production facility is the local security provided by the contractor, but we have not adequately incorporated security requirements into standard DLA contracts. If we do choose to write such requirements into DLA contracts in a more effective and meaningful way, who will have oversight to ensure that the contractor is meeting those requirements imposed upon him by law? Is that a military function, or is that a civilian function? If it is a civilian function, who does it? When we move beyond the contractor who owns the facility within the DIB, the next layer of protection has been assigned to civilian law enforcement—local, State, and Federal—and at the Federal level, principally the Department of Justice through the FBI. However, if an Al Qaeda attack is likely to exceed

the defensive capabilities of our law enforcement community, what do we do as a nation to ensure that we bring sufficient forces to bear in order to ensure the defeat of the enemy attack? I would argue that the next layer of defense is the National Guard under Title 32 status under the command of the governor, as we discussed earlier, at the expense of DoD and potentially commanded by a dual-hatted officer who could command both Title 10 and Title 32 forces.

Take this as a message of "tough love." In my judgment, the CIP community must move beyond the defense culture of the Cold War. I urge you to build upon your past success in defending our nation against the Soviet threat. Do not exclusively rely on concepts of single points of vulnerability and engineering analysis—these provide a good start, but it is only a start. Recognize that the terrorist threat is quite different. We now must deal not only with redundancy, but with the inescapable fact that there are transnational terrorists seeking to exploit our vulnerabilities. There are bad people out there; people whose targeting data on our facilities we have recovered. Our enemies are thorough, patient, methodical, and detailed in trying to identify the kinds of vulnerabilities that go beyond mere engineering concepts. They are diligently seeking the kinds of vulnerabilities that will provide them with the opportunity for reconnaissance, and after reconnaissance, with the opportunity to once again attack the United States within our borders. That is the reality of the asymmetric twenty-first century transnational threat.

Like our operational capabilities, like our intelligence capabilities, we must bring CIP fully into the twenty-first century. Abraham Lincoln said, "As our cause is new, so must we think and act anew." The defense of our critical infrastructure, like all other elements of our homeland defense, must be active, not passive. It must be equally effective against nation-states with nuclear weapons and terrorists with dirty bombs. It must seize and maintain the operational initiative. It must integrate all the elements of our national strength: the private sector, the public sector, local, state, and Federal governments. We all have a role to play. Building upon the engineering concepts, the redundancies, and the hardening capabilities developed during the Cold War, we must ask ourselves: have we translated those concepts and capabilities into an effective defense, not against the Soviet Union, but against Al Qaeda, and against whatever transnational terrorist threat will arise in the future to take its place?

Success in this endeavor is up to all of us, but most especially, you who are the dedicated professionals of the CIP community. We're counting on you.


Prudens
Futuri